We claim:

1. A computer program product embodied on computer readable media readable by a computing system in a computing environment, for enforcing security policy using style sheet processing, comprising:

an input document;

one or more stored policy enforcement objects, wherein each of said stored policy enforcement objects specifies a security policy to be associated with zero or more elements of said input document;

a Document Type Definition (DTD) corresponding to said input document, wherein said DTD has been augmented with one or more references to selected ones of said stored policy enforcement objects;

an augmented style sheet processor, wherein said augmented processor further comprises:

computer-readable program code means for loading said DTD;

computer-readable program code means for resolving each of said one or more references in said loaded DTD;

computer-readable program code means for instantiating said policy enforcement objects associated with said resolved references;

computer-readable program code means for executing selected ones of said instantiated policy enforcement objects during application of one or more style sheets to said input document, wherein a result of said computer-readable program code means for executing is an interim transient document reflecting said execution;

computer-readable program code means for generating one or more random encryption keys;

computer-readable program code means for encrypting selected elements of said interim transient document, wherein a particular one of said generated random encryption keys may be used to encrypt one or more of said selected elements, while leaving zero or more other elements of said interim transient document unencrypted;

computer-readable program code means for encrypting each of said one or more random encryption keys; and

computer-readable program code means for creating an encrypted output document comprising said zero or more other unencrypted elements, said selected encrypted elements, and said encrypted encryption keys;

computer-readable program code means for requesting, from a user or process on a client device, said encrypted output document, wherein said user or process is a member of a particular group authorized to view at least one of said selected encrypted elements;

computer-readable program code means for receiving said requested output document at said client device; and

an augmented document processor executed on said client device, comprising:

computer-readable program code means for contacting a clerk of said particular group for decryption of selected ones of said encrypted encryption keys; and

computer-readable program code means for decrypting said requested output document using said decrypted selected ones of said encrypted encryption keys, thereby creating a result document.

2. The computer program product according to Claim 1, further comprising computer-readable program code means for rendering said result document on said client device.

3. The computer program product according to Claim 1, wherein said interim transient document comprises one or more encryption tags identifying elements needing encryption.

4. The computer program product according to Claim 1, wherein said input document is specified in an Extensible Markup Language (XML) notation.

5. The computer program product according to Claim 4, wherein said result document is specified in said XML notation.

6. The computer program product according to Claim 1, wherein said stored policy enforcement objects further comprise computer-readable program code means for overriding a method for evaluating said elements of said input document, and wherein said computer-readable program code means for executing further comprises computer-readable program code means for executing said computer-readable program code means for overriding.

7. The computer program product according to Claim 6, wherein said style sheets are specified in an Extensible Stylesheet Language (XSL) notation.

8. The computer program product according to Claim 7, wherein said method is a value-of method of said XSL notation, and wherein said computer-readable program code means for overriding said value-of method is by subclassing said value-of method.

9. The computer program product according to Claim 6 or Claim 8, wherein:

said overridden method comprises:

computer-readable program code means for generating encryption tags; and

computer-readable program code means for inserting said generated encryption tags into said interim transient document to surround elements of said interim transient document which are determined to require encryption; and

said computer-readable program code means for encrypting selected elements encrypts those elements surrounded by said inserted encryption tags.

10. The computer program product according to Claim 2, wherein:

each of said instantiated policy enforcement objects further comprises:

a specification of a community that is authorized to view said elements associated with said security policy, said specification of said communities further comprising specification of at least one of: (1) one or more individual users or processes which are community members, and (2) one or more groups which are community members, wherein each of said groups comprises one or more individual users or processes; and

an encryption requirement for said elements associated with said security policy; and

wherein said particular group is specified as one of said community members.

11. The computer program product according to Claim 10, wherein said encryption requirement further comprises specification of an encryption algorithm.

12. The computer program product according to Claim 10, wherein said encryption requirement further comprises specification of an encryption algorithm strength value.

13. The computer program product according to Claim 10, wherein:

said computer-readable program code means for encrypting said encryption keys further comprises computer-readable program code means for encrypting a different version of each of said random encryption keys for each of said one or more members of each of zero or more of said communities which uses said encryption key, and wherein each of said different versions is encrypted using a public key of said community member for which said different version was encrypted.

14. The computer program product according to Claim 10, wherein said encryption requirement may have a null value to indicate that said specified security policy does not require encryption.

15. The computer program product according to Claim 1, wherein said computer-readable program code means for encrypting selected elements uses a cipher block chaining mode encryption process.

16. The computer program product according to Claim 13, further comprising:

computer-readable program code means for creating a key class for each unique community, wherein said key class is associated with each of said encrypted elements for which this unique community is an authorized viewer, and wherein said key class comprises: (1) a strongest encryption requirement of said associated encrypted elements; (2) an identifier of each of said members of said unique community; and (3) one of said different versions of said encrypted encryption key for each of said identified community members; and

wherein:

said computer-readable program code means for generating said one or more random encryption keys generates a particular one of said random encryption keys for each of said key classes, and wherein each of said different versions in a particular key class is encrypted from said generated encryption key generated for said key class; and

said computer-readable program code means for encrypting selected elements uses that one of said particular random encryption keys which was generated for said key class with which said selected element is associated.

17. The computer program product according to Claim 13, wherein:

said computer-readable program code means for decrypting said requested output document further comprises:

computer-readable program code means for expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

computer-readable program code means for determining one or more of said expanded communities of which said requesting user or process is one of said expanded group members;

computer-readable program code means for decrypting, for each of said determined communities, said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members, thereby creating a decrypted key for each of said determined communities; and

computer-readable program code means for decrypting selected ones of said encrypted elements in said requested output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for one of said determined communities; and

said computer-readable program code means for rendering further comprises:

computer-readable program code means for rendering said decrypted selected ones and said other unencrypted elements.

18. The computer program product according to Claim 17, wherein:

said computer-readable program code means for contacting said group clerk further comprises:

computer-readable program code means for locating said group clerk; and

computer-readable program code means for establishing a session between said client device and said group clerk;

said computer-readable program code means for decrypting said different version for each of said determined communities further comprises:

computer-readable program code means for digitally signing said different version by said requesting user or process, thereby creating a first digital signature;

computer-readable program code means for sending said first digital signature and said different version to said group clerk on said session;

computer-readable program code means for receiving said sent first digital signature and said different version by said group clerk;

computer-readable program code means for verifying said first digital signature by said group clerk;

computer-readable program code means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

computer-readable program code means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

computer-readable program code means for re-encrypting said decrypted different version using a public key of said requesting user or process, thereby creating a re-encrypted key;

computer-readable program code means for digitally signing said re-encrypted key by said group clerk, thereby creating a second digital signature;

computer-readable program code means for returning said second digital signature and said re-encrypted key from said group clerk to said client device on said session;

computer-readable program code means for receiving said second digital signature and said re-encrypted key at said client device;

computer-readable program code means for verifying said second digital signature at said client device; and

computer-readable program code means, operable on said client device, for decrypting said received re-encrypted key using a private key of said requesting user or process, creating said decrypted key; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said requested output document is executed at said client device using said decrypted key.

19. The computer program product according to Claim 13, wherein:

said computer-readable program code means for decrypting said requested output document further comprises:

computer-readable program code means for expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

computer-readable program code means for determining one or more of said expanded communities of which said requesting user or process is one of said expanded group members; and

computer-readable program code means for decrypting selected ones of said encrypted elements in said requested output document, wherein said selected ones of said encrypted elements are those which were encrypted for one of said determined communities; and

said computer-readable program code means for rendering further comprises:

computer-readable program code means for rendering said returned decrypted elements and said other unencrypted elements.

20. The computer program product according to Claim 19, wherein:

said computer-readable program code means for contacting said group clerk further comprises:

computer-readable program code means for locating said group clerk; and

computer-readable program code means for establishing a mutually-authenticated secure session between said client device and said group clerk; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said requested output document further comprises:

computer-readable program code means for locating said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members;

computer-readable program code means for sending said located different version to said group clerk, along with an element encrypted with said different version, on said secure session;

computer-readable program code means for receiving said sent different version and said element by said group clerk;

computer-readable program code means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

computer-readable program code means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

computer-readable program code means for decrypting said element using said decrypted different version; and

computer-readable program code means for returning said decrypted element from said group clerk to said client device on said secure session.

21. The computer program product according to Claim 16, wherein:

said computer-readable program code means for contacting said group clerk further comprises:

computer-readable program code means for locating said group clerk; and

computer-readable program code means for establishing a mutually-authenticated secure session between said client device and said group clerk;

said computer-readable program code means for decrypting said requested output document further comprises:

computer-readable program code means for expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

computer-readable program code means for determining one or more of said key classes which identify said requesting user or process as one of said expanded group members;

computer-readable program code means for decrypting, for each of said determined key classes, said different version of said random encryption key in said key class which was encrypted using said public key of said one member, wherein said computer-readable program code means for decrypting uses a private key of said one member which is associated with said public key which was used for encryption, thereby creating a decrypted key; and

computer-readable program code means for decrypting selected ones of said encrypted elements in said requested output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for said key class; and

said computer-readable program code means for rendering further comprises:

computer-readable program code means for rendering said decrypted selected ones and said other unencrypted elements.

22. The computer program product according to Claim 17, wherein:

said computer-readable program code means for contacting said group clerk further comprises:

computer-readable program code means for locating said group clerk; and

computer-readable program code means for establishing a mutually-authenticated secure session between said client device and said group clerk;

said computer-readable program code means for decrypting said different version for each of said determined communities further comprises:

computer-readable program code means for sending said different version to said group clerk on said secure session;

computer-readable program code means for receiving said sent different version by said group clerk;

computer-readable program code means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

computer-readable program code means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

computer-readable program code means for returning said decrypted different version from said group clerk to said client device on said secure session; and

computer-readable program code means for receiving said decrypted different version at said client device; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said requested output document is executed at said client device using said received decrypted different version.

23. The computer program product according to Claim 17, Claim 21, or Claim 22, wherein said computer-readable program code means for rendering further comprises computer-readable program code means for rendering a substitute text message for any of said selected encrypted elements in said requested output document which cannot be decrypted by said computer-readable program code means for decrypting said requested output document.

24. The computer program product according to Claim 19, wherein:

said computer-readable program code means for contacting said group clerk further comprises:

computer-readable program code means for locating said group clerk; and

computer-readable program code means for establishing a session between said client device and said group clerk; and

said computer-readable program code means for decrypting selected ones of said encrypted elements in said requested output document further comprises:

computer-readable program code means for locating said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members;

computer-readable program code means for digitally signing, by said requesting user or process, said located version and an element encrypted with said different version, thereby creating a first digital signature;

computer-readable program code means for sending said first digital signature, said located different version, and said element to said group clerk on said session;

computer-readable program code means for receiving said sent first digital signature, said different version, and said element by said group clerk;

computer-readable program code means for verifying said first digital signature by said group clerk;

computer-readable program code means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

computer-readable program code means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

computer-readable program code means for decrypting said element using said decrypted different version;

computer-readable program code means for re-encrypting said decrypted element using a public key of said requesting user or process, thereby creating a re-encrypted element;

computer-readable program code means for digitally signing said re-encrypted element by said group clerk, thereby creating a second digital signature;

computer-readable program code means for returning said second digital signature and said re-encrypted element from said group clerk to said client device on said session;

computer-readable program code means for receiving said second digital signature and said re-encrypted element at said client device; and

computer-readable program code means for verifying said second digital signature by said requesting user or process.

25. The computer program product according to Claim 1, wherein said DTD is replaced by a schema.

26. The computer program product according to Claim 10, wherein said encryption requirement further comprises specification of an encryption key length.

27. The computer program product according to Claim 9, wherein said inserted encryption tags may surround either values of said elements or values and tags of said elements.

28. A system for enforcing security policy using style sheet processing in a computing environment, comprising:

an input document;

one or more stored policy enforcement objects, wherein each of said stored policy enforcement objects specifies a security policy to be associated with zero or more elements of said input document;

a Document Type Definition (DTD) corresponding to said input document, wherein said DTD has been augmented with one or more references to selected ones of said stored policy enforcement objects;

an augmented style sheet processor, wherein said augmented processor further comprises:

means for loading said DTD;

means for resolving each of said one or more references in said loaded DTD;

means for instantiating said policy enforcement objects associated with said resolved references;

means for executing selected ones of said instantiated policy enforcement objects during application of one or more style sheets to said input document, wherein a result of said means for executing is an interim transient document reflecting said execution;

means for generating one or more random encryption keys;

means for encrypting selected elements of said interim transient document, wherein a particular one of said generated random encryption keys may be used to encrypt one or more of said selected elements, while leaving zero or more other elements of said interim transient document unencrypted;

means for encrypting each of said one or more random encryption keys; and

means for creating an encrypted output document comprising said zero or more other unencrypted elements, said selected encrypted elements, and said encrypted encryption keys;

means for requesting, from a user or process on a client device, said encrypted output document, wherein said user or process is a member of a particular group authorized to view at least one of said selected encrypted elements;

means for receiving said requested output document at said client device; and

an augmented document processor executed on said client device, comprising:

means for contacting a clerk of said particular group for decryption of selected ones of said encrypted encryption keys; and

means for decrypting said requested output document using said decrypted selected ones of said encrypted encryption keys, thereby creating a result document.

29. The system according to Claim 28, further comprising means for rendering said result document on said client device.

30. The system according to Claim 28, wherein said interim transient document comprises one or more encryption tags identifying elements needing encryption.

31. The system according to Claim 28, wherein said input document is specified in an Extensible Markup Language (XML) notation.

32. The system according to Claim 31, wherein said result document is specified in said XML notation.

33. The system according to Claim 28, wherein said stored policy enforcement objects further comprise means for overriding a method for evaluating said elements of said input document, and wherein said means for executing further comprises means for executing said means for overriding.

34. The system according to Claim 33, wherein said style sheets are specified in an Extensible Stylesheet Language (XSL) notation.

35. The system according to Claim 34, wherein said method is a value-of method of said XSL notation, and wherein said means for overriding said value-of method is by subclassing said value-of method.

36. The system according to Claim 33 or Claim 35, wherein:

said overridden method comprises:

means for generating encryption tags; and

means for inserting said generated encryption tags into said interim transient document to surround elements of said interim transient document which are determined to require encryption; and

said means for encrypting selected elements encrypts those elements surrounded by said inserted encryption tags.

37. The system according to Claim 29, wherein:

each of said instantiated policy enforcement objects further comprises:

a specification of a community that is authorized to view said elements associated with said security policy, said specification of said communities further comprising specification of at least one of: (1) one or more individual users or processes which are community members, and

(2) one or more groups which are community members, wherein each of said groups comprises one or more individual users or processes; and

an encryption requirement for said elements associated with said security policy; and

wherein said particular group is specified as one of said community members.

38. The system according to Claim 37, wherein said encryption requirement further comprises specification of an encryption algorithm.

39. The system according to Claim 37, wherein said encryption requirement further comprises specification of an encryption algorithm strength value.

40. The system according to Claim 37, wherein:

said means for encrypting said encryption keys further comprises means for encrypting a different version of each of said random encryption keys for each of said one or more members of each of zero or more of said communities which uses said encryption key, and wherein each of said different versions is encrypted using a public key of said community member for which said different version was encrypted.

41. The system according to Claim 37, wherein said encryption requirement may have a null value to indicate that said specified security policy does not require encryption.

42. The system according to Claim 28, wherein said means for encrypting selected elements uses a cipher block chaining mode encryption process.

43. The system according to Claim 40, further comprising:

means for creating a key class for each unique community, wherein said key class is associated with each of said encrypted elements for which this unique community is an authorized viewer, and wherein said key class comprises: (1) a strongest encryption requirement of said associated encrypted elements; (2) an identifier of each of said members of said unique community; and (3) one of said different versions of said encrypted encryption key for each of said identified community members; and

wherein:

said means for generating said one or more random encryption keys generates a particular one of said random encryption keys for each of said key classes, and wherein each of said different versions in a particular key class is encrypted from said generated encryption key generated for said key class; and

said means for encrypting selected elements uses that one of said particular random encryption keys which was generated for said key class with which said selected element is associated.

44. The system according to Claim 40, wherein:

said means for decrypting said requested output document further comprises:

means for expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

means for determining one or more of said expanded communities of which said requesting user or process is one of said expanded group members;

means for decrypting, for each of said determined communities, said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members, thereby creating a decrypted key for each of said determined communities; and

means for decrypting selected ones of said encrypted elements in said requested output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for one of said determined communities; and

said means for rendering further comprises:

means for rendering said decrypted selected ones and said other unencrypted elements.

45. The system according to Claim 44, wherein:

said means for contacting said group clerk further comprises:

means for locating said group clerk; and

means for establishing a session between said client device and said group clerk;

said means for decrypting said different version for each of said determined communities further comprises:

means for digitally signing said different version by said requesting user or process, thereby creating a first digital signature;

means for sending said first digital signature and said different version to said group clerk on said session;

means for receiving said sent first digital signature and said different version by said group clerk;

means for verifying said first digital signature by said group clerk;

means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

means for re-encrypting said decrypted different version using a public key of said requesting user or process, thereby creating a re-encrypted key;

means for digitally signing said re-encrypted key by said group clerk, thereby creating a second digital signature;

means for returning said second digital signature and said re-encrypted key from said group clerk to said client device on said session;

means for receiving said second digital signature and said re-encrypted key at said client device;

means for verifying said second digital signature at said client device; and

means, operable on said client device, for decrypting said received re-encrypted key using a private key of said requesting user or process, creating said decrypted key; and

said means for decrypting selected ones of said encrypted elements in said requested output document is executed at said client device using said decrypted key.

46. The system according to Claim 40, wherein:

said means for decrypting said requested output document further comprises:

means for expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

means for determining one or more of said expanded communities of which said requesting user or process is one of said expanded group members; and

means for decrypting selected ones of said encrypted elements in said requested output document, wherein said selected ones of said encrypted elements are those which were encrypted for one of said determined communities; and

said means for rendering further comprises:

means for rendering said returned decrypted elements and said other unencrypted elements.

47. The system according to Claim 46, wherein:

said means for contacting said group clerk further comprises:

means for locating said group clerk; and

means for establishing a mutually-authenticated secure session between said client device and said group clerk; and

said means for decrypting selected ones of said encrypted elements in said requested output document further comprises:

means for locating said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members;

means for sending said located different version to said group clerk, along with an element encrypted with said different version, on said secure session;

means for receiving said sent different version and said element by said group clerk;

means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

means for decrypting said element using said decrypted different version; and

means for returning said decrypted element from said group clerk to said client device on said secure session.

48. The system according to Claim 43, wherein:

said means for contacting said group clerk further comprises:

means for locating said group clerk; and

means for establishing a mutually-authenticated secure session between said client device and said group clerk;

said means for decrypting said requested output document further comprises:

means for expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

means for determining one or more of said key classes which identify said requesting user or process as one of said expanded group members;

means for decrypting, for each of said determined key classes, said different version of said random encryption key in said key class which was encrypted using said public key of said one member, wherein said means for decrypting uses a private key of said one member which is associated with said public key which was used for encryption, thereby creating a decrypted key; and

means for decrypting selected ones of said encrypted elements in said requested output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for said key class; and

said means for rendering further comprises:

means for rendering said decrypted selected ones and said other unencrypted elements.

49. The system according to Claim 44, wherein:

said means for contacting said group clerk further comprises:

means for locating said group clerk; and

means for establishing a mutually-authenticated secure session between said client device and said group clerk;

said means for decrypting said different version for each of said determined communities further comprises:

means for sending said different version to said group clerk on said secure session;

means for receiving said sent different version by said group clerk;

means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

means for returning said decrypted different version from said group clerk to said client device on said secure session; and

means for receiving said decrypted different version at said client device; and

said means for decrypting selected ones of said encrypted elements in said requested output document is executed at said client device using said received decrypted different version.

50. The system according to Claim 44, Claim 48, or Claim 49, wherein said means for rendering further comprises means for rendering a substitute text message for any of said selected encrypted elements in said requested output document which cannot be decrypted by said means for decrypting said requested output document.

51. The system according to Claim 46, wherein:

said means for contacting said group clerk further comprises:

means for locating said group clerk; and

means for establishing a session between said client device and said group clerk; and

said means for decrypting selected ones of said encrypted elements in said requested output document further comprises:

means for locating said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members;

means for digitally signing, by said requesting user or process, said located version and an element encrypted with said different version, thereby creating a first digital signature;

means for sending said first digital signature, said located different version, and said element to said group clerk on said session;

means for receiving said sent first digital signature, said different version, and said element by said group clerk;

means for verifying said first digital signature by said group clerk;

means for verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

means for decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

means for decrypting said element using said decrypted different version;

means for re-encrypting said decrypted element using a public key of said requesting user or process, thereby creating a re-encrypted element;

means for digitally signing said re-encrypted element by said group clerk, thereby creating a second digital signature;

means for returning said second digital signature and said re-encrypted element from said group clerk to said client device on said session;

means for receiving said second digital signature and said re-encrypted element at said client device; and

means for verifying said second digital signature by said requesting user or process.

52. The system according to Claim 28, wherein said DTD is replaced by a schema.

53. The system according to Claim 37, wherein said encryption requirement further comprises specification of an encryption key length.

54. The system according to Claim 36, wherein said inserted encryption tags may surround either values of said elements or values and tags of said elements.

55. A method for enforcing security policy using style sheet processing, comprising the steps of:

providing an input document;

providing one or more stored policy enforcement objects, wherein each of said stored policy enforcement objects specifies a security policy to be associated with zero or more elements of said input document;

providing a Document Type Definition (DTD) corresponding to said input document, wherein said DTD has been augmented with one or more references to selected ones of said stored policy enforcement objects;

executing an augmented style sheet processor, further comprising the steps of:

loading said DTD;

resolving each of said one or more references in said loaded DTD;

instantiating said policy enforcement objects associated with said resolved references;

executing selected ones of said instantiated policy enforcement objects during application of one or more style sheets to said input document, wherein a result of said step of executing selected ones is an interim transient document reflecting said execution;

generating one or more random encryption keys;

encrypting selected elements of said interim transient document, wherein a particular one of said generated random encryption keys may be used to encrypt one or more of said selected elements, while leaving zero or more other elements of said interim transient document unencrypted;

encrypting each of said one or more random encryption keys; and

creating an encrypted output document comprising said zero or more other unencrypted elements, said selected encrypted elements, and said encrypted encryption keys;

requesting, from a user or process on a client device, said encrypted output document, wherein said user or process is a member of a particular group authorized to view at least one of said selected encrypted elements;

receiving said requested output document at said client device; and

executing an augmented document processor on said client device, further comprising the steps of:

contacting a clerk of said particular group for decryption of selected ones of said encrypted encryption keys; and

decrypting said requested output document using said decrypted selected ones of said encrypted encryption keys, thereby creating a result document.

56. The method according to Claim 55, further comprising the step of rendering said result document on said client device.

57. The method according to Claim 55, wherein said interim transient document comprises one or more encryption tags identifying elements needing encryption.

58. The method according to Claim 55, wherein said input document is specified in an Extensible Markup Language (XML) notation.

59. The method according to Claim 58, wherein said result document is specified in said XML notation.

60. The method according to Claim 55, wherein said stored policy enforcement objects further comprise executable code for overriding a method for evaluating said elements of said input document, and wherein said executing selected ones step further comprises overriding said method for evaluating.

61. The method according to Claim 60, wherein said style sheets are specified in an Extensible Stylesheet Language (XSL) notation.

62. The method according to Claim 61, wherein said method is a value-of method of said XSL notation, and wherein said step of overriding said value-of method is by subclassing said value-of method.

63. The method according to Claim 60 or Claim 62, wherein:

said step of overriding further comprises the steps of:

generating encryption tags; and

inserting said generated encryption tags into said interim transient document to surround elements of said interim transient document which are determined to require encryption; and

said step of encrypting selected elements encrypts those elements surrounded by said inserted encryption tags.

64. The method according to Claim 56, wherein:

each of said instantiated policy enforcement objects further comprises:

a specification of a community that is authorized to view said elements associated with said security policy, said specification of said communities further comprising specification of at least one of: (1) one or more individual users or processes which are community members, and (2) one or more groups which are community members, wherein each of said groups comprises one or more individual users or processes; and

an encryption requirement for said elements associated with said security policy; and

wherein said particular group is specified as one of said community members.

65. The method according to Claim 64, wherein said encryption requirement further comprises specification of an encryption algorithm.

66. The method according to Claim 64, wherein said encryption requirement further comprises specification of an encryption algorithm strength value.

67. The method according to Claim 64, wherein:

said step of encrypting said encryption keys further comprises the step of encrypting a different version of each of said random encryption keys for each of said one or more members of each of zero or more of said communities which uses said encryption key, and wherein each of

said different versions is encrypted using a public key of said community member for which said different version was encrypted.

68. The method according to Claim 64, wherein said encryption requirement may have a null value to indicate that said specified security policy does not require encryption.

69. The method according to Claim 55, wherein said step of encrypting selected elements uses a cipher block chaining mode encryption process.

70. The method according to Claim 67, further comprising the step of:

creating a key class for each unique community, wherein said key class is associated with each of said encrypted elements for which this unique community is an authorized viewer, and wherein said key class comprises: (1) a strongest encryption requirement of said associated encrypted elements; (2) an identifier of each of said members of said unique community; and (3) one of said different versions of said encrypted encryption key for each of said identified community members; and

wherein:

said step of generating said one or more random encryption keys generates a particular one of said random encryption keys for each of said key classes, and wherein each of said different versions in a particular key class is encrypted from said generated encryption key generated for said key class; and

said step of encrypting selected elements uses that one of said particular random encryption keys which was generated for said key class with which said selected element is associated.

71. The method according to Claim 67, wherein:

said step of decrypting said requested output document further comprises the steps of:

expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

determining one or more of said expanded communities of which said requesting user or process is one of said expanded group members;

decrypting, for each of said determined communities, said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members, thereby creating a decrypted key for each of said determined communities; and

decrypting selected ones of said encrypted elements in said requested output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for one of said determined communities; and

said step of rendering further comprises the step of:

rendering said decrypted selected ones and said other unencrypted elements.

72. The method according to Claim 71, wherein:

said step of contacting said group clerk further comprises the steps of:

locating said group clerk; and

establishing a session between said client device and said group clerk;

said step of decrypting said different version for each of said determined communities further comprises the steps of:

digitally signing said different version by said requesting user or process, thereby creating a first digital signature;

sending said first digital signature and said different version to said group clerk on said session;

receiving said sent first digital signature and said different version by said group clerk;

verifying said first digital signature by said group clerk;

verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

re-encrypting said decrypted different version using a public key of said requesting user or process, thereby creating a re-encrypted key;

digitally signing said re-encrypted key by said group clerk, thereby creating a second digital signature;

returning said second digital signature and said re-encrypted key from said group clerk to said client device on said session;

receiving said second digital signature and said re-encrypted key at said client device;

verifying said second digital signature at said client device; and

decrypting, at said client device, said received re-encrypted key using a private key of said requesting user or process, creating said decrypted key; and

said step of decrypting selected ones of said encrypted elements in said requested output document is executed at said client device using said decrypted key.

73. The method according to Claim 67, wherein:

said step of decrypting said requested output document further comprises the steps of:

expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

determining one or more of said expanded communities of which said requesting user or process is one of said expanded group members; and

decrypting selected ones of said encrypted elements in said requested output document, wherein said selected ones of said encrypted elements are those which were encrypted for one of said determined communities; and

said step of rendering further comprises the step of:

rendering said returned decrypted elements and said other unencrypted elements.

74. The method according to Claim 73, wherein:

said step of contacting said group clerk further comprises the steps of:

locating said group clerk; and

establishing a mutually-authenticated secure session between said client device and said group clerk; and

said step of decrypting selected ones of said encrypted elements in said requested output document further comprises the steps of:

locating said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members;

sending said located different version to said group clerk, along with an element encrypted with said different version, on said secure session;

receiving said sent different version and said element by said group clerk;

verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

decrypting said element using said decrypted different version; and

returning said decrypted element from said group clerk to said client device on said secure session.

75. The method according to Claim 70, wherein:

said step of contacting said group clerk further comprises the steps of:

locating said group clerk; and

establishing a mutually-authenticated secure session between said client device and said group clerk;

said step of decrypting said requested output document further comprises the steps of:

expanding said one or more groups of said communities to determine said individual users or processes in each of said expanded groups;

determining one or more of said key classes which identify said requesting user or process as one of said expanded group members;

decrypting, for each of said determined key classes, said different version of said random encryption key in said key class which was encrypted using said public key of said one member, wherein said step of decrypting uses a private key of said one member which is associated with said public key which was used for encryption, thereby creating a decrypted key; and

decrypting selected ones of said encrypted elements in said requested output document using said decrypted keys, wherein said selected ones of said encrypted elements are those which were encrypted for said key class; and

said step of rendering further comprises the step of:

rendering said decrypted selected ones and said other unencrypted elements.

76. The method according to Claim 71, wherein:

said step of contacting said group clerk further comprises the steps of:

locating said group clerk; and

establishing a mutually-authenticated secure session between said client device and said group clerk;

said step of decrypting said different version for each of said determined communities further comprises the steps of:

sending said different version to said group clerk on said secure session;

receiving said sent different version by said group clerk;

verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

returning said decrypted different version from said group clerk to said client device on said secure session; and

receiving said decrypted different version at said client device; and

said step of decrypting selected ones of said encrypted elements in said requested output document is executed at said client device using said received decrypted different version.

77. The method according to Claim 71, Claim 75, or Claim 76, wherein said step of rendering further comprises the step of rendering a substitute text message for any of said selected encrypted elements in said requested output document which cannot be decrypted by said step of decrypting said requested output document.

78. The method according to Claim 73, wherein:

said step of contacting said group clerk further comprises the steps of:

locating said group clerk; and

establishing a session between said client device and said group clerk; and

said step of decrypting selected ones of said encrypted elements in said requested output document further comprises the steps of:

locating said different version of said random encryption key which was encrypted using said public key of said one member, wherein said one member is said expanded group of which said requesting user or process is one of said expanded group members;

digitally signing, by said requesting user or process, said located version and an element encrypted with said different version, thereby creating a first digital signature;

sending said first digital signature, said located different version, and said element to said group clerk on said session;

receiving said sent first digital signature, said different version, and said element by said group clerk;

verifying said first digital signature by said group clerk;

verifying, by said group clerk, that said requesting user or process is one of said authorized members of said determined community associated with said different version;

decrypting said different version using a private key of said one member which is associated with said public key which was used for encryption;

decrypting said element using said decrypted different version;

re-encrypting said decrypted element using a public key of said requesting user or process, thereby creating a re-encrypted element;

digitally signing said re-encrypted element by said group clerk, thereby creating a second digital signature;

returning said second digital signature and said re-encrypted element from said group clerk to said client device on said session;

receiving said second digital signature and said re-encrypted element at said client device; and

verifying said second digital signature by said requesting user or process.

79. The method according to Claim 55, wherein said DTD is replaced by a schema.

80. The method according to Claim 64, wherein said encryption requirement further comprises specification of an encryption key length.

81. The method according to Claim 63, wherein said inserted encryption tags may surround either values of said elements or values and tags of said elements.